Sign In »
New user? Register Now! Help
Gene6 FTP Server Forums Members Calendar
Gene6 FTP Server Forum > Gene6 FTP Server > Support > How to
Board Guidelines View New Content
Page 1 of 1
You cannot reply to this topic You cannot start a new topic

Hardening your FTP Server

Security checks and ideas

Rate Topic: 1 Votes

Matthieu #1

Gene6
Addicted Member
G6 STAFF
Group: Staff
Posts: 1964
Joined: 22-October 03
Gender: Male
Location: France : Mouy
Interests: Science-fiction, World news

Posted 02 March 2005 - 05:39 PM

If you are unsure that you have setup your server correctly, or if you are searching for ideas on how to make it more armored, here is a suggested checklist :

Past fixed security reports

Always make sure you are running the latest version!

2005-03-09 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0690 (modified since v3.5)
2006-05-03 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2172 (fixed since v3.8)

Administration / Properties

- Grant all access to localhost : should be only checked for initial server setup, then once you have created an administrator account, uncheck it to disable local user access (should be already off in a multi-users environment).

Administration / IP binding

- Default administration port is 8021, you can change it to a different value. Do not forget to also change the server profile in the administration client.

Domain / Authentication

- Max. login sequences : default to 3, after 3 trials of USER/PASS sequence the user will be disconnected
- Login error delay : default to 3 seconds, if you have many unexpected connection attempts you can increase to 10s (this will also delay users not entering good login/password because of typo ...)
- Redirect wrong login : can be used to cheat a robot into thinking it has found a good login/password whereas he's logged under the anonymous account.

Domain / Miscellaneous

- Anti hammer : if you have angry people knocking at the server doors, enable the anti hammer and see them becoming automatically banned for annoying you.

Domain / Logs and reports

- Defining a new regular log can show you what is going on on your server, for example you can enable "login", "upload", "download", "file deletion" only to have a quick view of what your users are doing.

Domain / Secure / Options

- Enable "Block banned IP" so the client does not receive any message knowing why he's banned, he'll just think there is a server problem.

Domain / IP binding

- Running the server on a non standard port like 10021, 20121 ... can hide you from automated scripts searching for public writable FTP servers.
- Using SSL will encrypt all data that is exchanged between the server and the client.

User account

- If you need an anonymous account, never allow read and write access to the same folder with an anonymous

account.
- Using built in password generator will produce 8 random chars passwords, thus it is harder to guess the password using brute forcing (it is copied to clipboard).
- "Regular password stored as MD5" stores a hashed value of the entered password, it can't be decrypted (only by brute forcing).
- Enable "Secure connection only (ssl)" for sensitive accounts containing important data, the user will be forced to use an encrypted connection or the server will not log him. You can as well require that the user uses SSL for some directory access (see access rights).
- Set an expiration date for temporary accounts, so you do not forget to disable them later and leave a potential entry door.

User account / Advanced

- If you do not want your user to have access to certain ftp commands, then disable them : see Advanced / Disabled commands (STOR, XCRC, XMD5 ...)
- FXP, server to server should be disabled (by default), except if you expect the user to transfer from/to another server.

User account / Banned files

- Define forbidden files filters on your server, like *.vbs, *.bat, *.exe

User account / Time of day access

- As a company you may only allow access to your server during office hours, define the hour range.

User account / IP access

- If required, define the IP access to only allow known hosts/ip (if possible), so if you know your users always come from *.thissubnet.com, then just add in the user account a rule "+*.thissubnet.com", this also works with ip or dynamic names (enter them between parenthesis "+(bobftp.dyndns.org)").
You can also set IP access at domain, FTP Server level or Administration level.

Service account

Under Windows XP/2003, you can use the new network service account named NETWORK SERVICE instead of LOCAL SYSTEM to increase the server security and reduce access rights of the server process, 2 steps are required :

1) changing service account :

- launch Start / Run / services.msc
- scroll to "Gene6 FTP Server", right click to open the properties page, click on "Log on"
- select "This account" and click Browse
- "Select this object type" should be "User or Built-in security principal"
- click on "Advanced"
- click on "Find now"
- in the list select "NETWORK SERVICE"
- click on OK
- click on OK to validate the "Select user" window choice
- clear the password boxes, then click on OK
- restart the Service when prompted

2) allowing NETWORK SERVICE read/write access to Gene6 FTP Server configuration files :

- open Explorer and browse to c:\Program Files\Gene6 FTP Server\
- right click, open Properties page
- in page "Securities", add NETWORK SERVICE with full control
- restart the service to apply changes immediately or wait for the cache to refresh

Restricting available SSL ciphers

You can specify which ciphers to use by adding a line in [Domain] section of you domains settings.ini file.

For instance, to only allow AES256-SHA cipher, add this line in your domain settings.ini file :

CODE
SSLCipherList=AES256-SHA

FTP clients that do not support this cipher won't be able to do SSL handshake with the server.

If you want to allow a list of ciphers, separate them by a colon :

CODE
SSLCipherList=AES256-SHA:RC4-MD5

Do not hesitate to post your suggestions to increase security.

Gene6, SARL
Do not use PM to ask for support, use the forum or support email.

Special offer : 10% discount with coupon code : **DISCOUNT**

0

|— How to Go

Share this topic:

← Previous Topic | How to | Next Topic →

Page 1 of 1

You cannot reply to this topic You cannot start a new topic

1 User(s) are reading this topic
0 members, 1 guests, 0 anonymous users

English (USA) Go

Time Now: May 06 2014 10:24 PM

Back To Top Forum Home Delete My Cookies Mark Board As Read

Community Forum Software by IP.Board
Licensed to: Gene6 SARL